

# Data Privacy Impact Assessment

**Name of Academy/Trust:** Leger Education Trust (Campsmount Academy, Spa Academy, Littlemoor Infant Academy, Moss Road Infant Academy).

**Pupils On Roll:** 1299

**Staff On Roll:** 171 FTE

**Data Action/Project:** To ensure that data protection principles are adhered to when staff are working remotely e.g. home. This is to ensure that data security procedures are followed, in order to minimise a data breach.

**Data Protection Officer:** Tim Pinto

**Data Protection Lead:** Rebecca Grange, Director of Operations

**Date:** 27/01/21

## 1. RISK ANALYSIS OF DATA PROJECT

Aim of project	The aim relates to the security of data when staff are working offsite. Many staff work from home to undertake school based tasks. With the emergence of Covid 19 many staff now undertake tasks associated to the use of electronic and paper data.
Why does a DPIA need to be completed?	Within the school environment, there is greater security measures in place to protect data. Offsite working brings more challenges related to the safety of electronic and paper data.

## 2. DATA PROTECTION PROCEDURES

Why is this a high risk?	Staff working offsite has become necessary due to emergency measures implemented during the Covid-19 pandemic and it is essential to support students to further their education
Are there legal implications?	Directives from the Department of Education (October 22).
How will the data be processed?	Teachers process thousands of pieces of personal data during their normal teaching day. Some of this will include special category data such as medical and ethnicity and religion. Administration staff will be looking at new intake data as well as staff payroll and HR information.
Will the processing include personal/sensitive data?	Present on school systems is every possible form of personal data including special category data.
What type of data is included?	Personal data and special categories of data.
Does it include children's data?	Yes
Does it include data for vulnerable children?	Yes
Where is the data stored?	All Trust IT networks have safeguards against data hijack/terrorism including bolt on solution from SOPHOS. No data stored on workstations, stored on OneDrive,

	SharePoint or network. All servers have X-Protect which prevents an executable file being run without permission. If ransomware payload tries to activate, the executable portion of that is unable to run. SOPHOS have advised that this is fully functional. The structure of the files on the server is such that an attack is limited to one directory. Web filter with Barracuda Technologies. Web security gateway. Filters on content, web applications. Filters at SSL level. Generates and stores log files. Content filters updated automatically weekly. Data stored internally on Storage Area Network (SAN) through an array of discs. Configured so that data cannot be lost. Backed up each night to Network Attached Storage (NAS). Littlemoor/Moss Road - off site storage through DMBC or ACS.
What are the data relationships?	Various combinations of relationships exist between school, student, employee, parents, leavers, sub-contract staff.
Will the rights of data subjects be compromised?	Associated risks (and ways to reduce risk) have been set out in sections 5/6.
Have issues around the use of electronic data been assessed?	Risk assessments – cyber security; risk registers for academies and Trust; training.
Have issues around the use of paper data been assessed?	Staff are asked to only take essential paper data offsite and must be signed out.
Are any other data actions involved?	Use of electronic systems to amend and update data sets.
Have data risks been addressed?	See section 5/6.

### 3. CONSULTATION PROCESS

How have individuals' views been sought?	We have contacted all parents via email and letter regarding the use of new remote learning.
Have governors been briefed?	Weekly briefings to governors include remote learning updates.
Are other processors involved?	Yes, we will seek assistance from any data processors that are included in events where staff access data remotely.

### 4. DATA NECESSITY AND PROPORTIONALITY

What is your lawful basis for processing?	This will be done under a public task and also the legal responsibility (see DfE directive (Oct 2020).
Does the processing actually achieve your purpose?	Yes, it will deliver online sessions to pupils and also direct tuition sessions to bespoke pupils.
Is there another way to achieve the same outcome?	Due to the pandemic, only specific pupils are allowed into school. Remote learning is a vital way for them to continue their education.
How will you prevent function creep? This means the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, which may lead to potential invasion of privacy.	This is not known at present.

How will you ensure data quality and data minimisation?	N/A.
What information will you give individuals?	Staff have been briefed on the safeguarding and data protection risks and would inform SLT if there was any issue when working offsite.
How will you help to support their rights?	The DPO regular reminds schools/trusts about their obligations of protecting data when working offsite.
What measures do you take to ensure processors comply?	N/A
How do you safeguard any international transfers?	N/A

## 5. IDENTITY AND ASSESS RISKS

This looks at the potential risks associated on individuals.

No:	Risk if paper or electronic systems containing personal data are accessed by unauthorised persons	Likelihood of harm	Severity of harm	Overall risk
1	Unencrypted devices used	Possible	Significant	High
2	Others having access to devices	Possible	Significant	High
3	Loss of device	Possible	Significant	High
4	Divulging personal data to others	Probable	Significant	High
5	Breaches not reported	Probable	Significant	High
6	Teachers' mark sheets and records	Possible	Minimal	Low
7	Safeguarding information	Probable	Severe	High
8	SEN and FSM data	Possible	Significant	High
9	Staff, parent and governor records	Possible	Significant	High
10	Paper or electronic storage mishandled	Probable	Severe	High


## 6. IDENTIFY MEASURES TO REDUCE RISK

This looks at ways to reduce risk set out in Section 5

No:	Options to reduce risk or eliminate risk	Effect on risk	Residual Risk	Measure communicated
1	<b>Unencrypted devices used</b> Staff should check with the IT technician that there device is secured and know how to access any remote learning tools.	Reduced	Medium	Yes
2	<b>Others having access to devices</b> Staff should use work devices (where possible) and ensure that they follow procedures to ensure that no other individuals are able to access school based data.	Reduced	Medium	Yes
3	<b>Loss of device</b> It is important that staff ensure that school devices are kept securely offsite and follow the data breach procedures if it is lost.	Reduced	Low	Yes
4	<b>Divulging personal data to others</b> Staff should only divulge a minimum amount of information and if asked to share further data, they should speak to SLT/DPO.	Reduced	Low	Yes

5	<b>Breaches not reported</b> Staff should be reminded regularly about data breaches and that they should report them immediately to SLT.	Reduced	Medium	Yes
6	<b>Teachers' mark sheets and records</b> These should be kept in the possession of teachers/staff and held securely when taken offsite.	Reduced	Low	Yes
7	<b>Safeguarding information</b> If staff are using any electronic system, they must ensure that they log off securely after use. Paper data must only be taken offsite in extreme circumstances.	Reduced	Medium	Yes
8	<b>SEN and FSM data</b> [As 7]	Reduced	Medium	Yes
9	<b>Staff, parent and governor records</b> As [6]	Reduced	Medium	Yes
10	<b>Paper or electronic storage mishandled</b> Staff should only take essential data offsite and discuss with SLT regarding the reasons why they have to take this data offsite.	Reduced	Medium	Yes

## 7. STEP 7: SIGN OFF AND RECORD OUTCOMES

Position:	Name:	Signed:
Chief Executive	Adam Dale	
Chair of Directors:	Babs Lynds	
IT Manager:	Simon Nicholson	
DP Lead	Rebecca Grange	
DPO:	Tim Pinto	